



PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Docket No: Q78254

Damien GALAND

Appln. No.: 10/705,837

Group Art Unit: Not Assigned

Confirmation No.: Not Assigned

Examiner: Not Assigned

Filed: November 13, 2003

For: NETWORK LEVEL ADMISSION CONTROL APPARATUS FOR A
COMMUNICATIONS NETWORK HAVING A SUB-IP LEVEL PROTOCOL

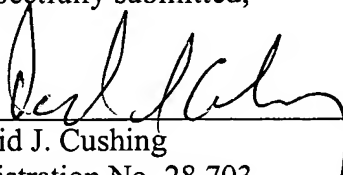
SUBMISSION OF PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is a certified copy of the priority document on which a claim to
priority was made under 35 U.S.C. § 119. The Examiner is respectfully requested to
acknowledge receipt of said priority document.

Respectfully submitted,


David J. Cushing
Registration No. 28,703

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Enclosures: France 0214227

Date: April 27, 2004



Q78254
181

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 30 OCT. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DS 543 W 400899

| | | | |
|---|----------------------|--|---------------------------|
| REMISE DES PIÈCES DATE: 14 NOV 2002 LIEU: 75 INPI PARIS N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI: 0214227 DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI: 14 NOV. 2002 | | 1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE COMPAGNIE FINANCIERE ALCATEL Département PI Sylvain CHAFFRAIX 30 avenue Kléber 75116 PARIS | |
| Vos références pour ce dossier (facultatif) 104572/SYC/NBND/TPM | | | |
| Confirmation d'un dépôt par télécopie <input type="checkbox"/> N° attribué par l'INPI à la télécopie | | | |
| 2 NATURE DE LA DEMANDE | | Cochez l'une des 4 cases suivantes | |
| Demande de brevet | | <input checked="" type="checkbox"/> | |
| Demande de certificat d'utilité | | <input type="checkbox"/> | |
| Demande divisionnaire | | <input type="checkbox"/> | |
| Demande de brevet initiale | | N° | Date <input type="text"/> |
| ou demande de certificat d'utilité initiale | | N° | Date <input type="text"/> |
| Transformation d'une demande de brevet européen | | <input type="checkbox"/> | Date <input type="text"/> |
| 3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) DISPOSITIF DE CONTROLE D'ADMISSION DE NIVEAU RESEAU POUR UN RESEAU DE COMMUNICATIONS A PROTOCOLE DE NIVEAU SOUS-IP | | | |
| 4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE | | Pays ou organisation _____ N° _____ Date <input type="text"/> / <input type="text"/> / <input type="text"/> Pays ou organisation _____ N° _____ Date <input type="text"/> / <input type="text"/> / <input type="text"/> Pays ou organisation _____ N° _____ Date <input type="text"/> / <input type="text"/> / <input type="text"/> <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite» | |
| 5 DEMANDEUR | | <input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite» | |
| Nom ou dénomination sociale | | ALCATEL | |
| Prénoms | | | |
| Forme juridique | | Société Anonyme | |
| N° SIREN | | 5.4.2.0.1.9.0.9.6 | |
| Code APE-NAF | | | |
| Adresse | Rue | 54, rue La Boétie | |
| | Code postal et ville | 75008 PARIS | |
| Pays | | FRANCE | |
| Nationalité | | Française | |
| N° de téléphone (facultatif) | | | |
| N° de télécopie (facultatif) | | | |
| Adresse électronique (facultatif) | | | |



BREVET D'INVENTION CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

| | | | |
|--|----------------------|--|-------|
| REMISE DES PIÈCES DATE: 14 NOV 2002 LIEU: 75 INPI PARIS N° D'ENREGISTREMENT: 0214227 NATIONAL ATTRIBUÉ PAR L'INPI | | Réservé à l'INPI | |
| Vos références pour ce dossier : <i>(facultatif)</i> | | 104572/SYC/NBND/TPM | |
| 6 MANDATAIRE | | | |
| Nom | | CHAFFRAIX | |
| Prénom | | Sylvain | |
| Cabinet ou Société | | Compagnie Financière Alcatel | |
| N° de pouvoir permanent et/ou de lien contractuel | | PG 9222 | |
| Adresse | Rue | 30 Avenue Kléber | |
| | Code postal et ville | 75116 | PARIS |
| N° de téléphone <i>(facultatif)</i> | | | |
| N° de télécopie <i>(facultatif)</i> | | | |
| Adresse électronique <i>(facultatif)</i> | | | |
| 7 INVENTEUR (S) | | | |
| Les inventeurs sont les demandeurs | | <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée | |
| 8 RAPPORT DE RECHERCHE | | Uniquement pour une demande de brevet (y compris division et transformation) | |
| Établissement immédiat ou établissement différé | | <input checked="" type="checkbox"/> <input type="checkbox"/> | |
| Paiement échelonné de la redevance | | Paiement en trois versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non | |
| 9 RÉDUCTION DU TAUX DES REDEVANCES | | Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence): | |
| Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes | | | |
| 10 SIGNATURE XXXXXXXXXX DU MANDATAIRE (Nom et qualité du signataire) | | VISA DE LA PRÉFECTURE OU DE L'INPI L. MARIELLO | |

Sylvain CHAFFRAIX / LC 40 B

DISPOSITIF DE CONTRÔLE D'ADMISSION DE NIVEAU RÉSEAU POUR UN RÉSEAU DE COMMUNICATIONS À PROTOCOLE DE NIVEAU SOUS-IP

5

L'invention concerne le domaine des communications entre terminaux via des réseaux de communications, et plus particulièrement le contrôle de la continuité d'un service dans le cas de communications impliquant des réseaux de types différents.

10

L'établissement d'une communication entre deux terminaux distants s'effectue souvent par l'intermédiaire de plusieurs réseaux de communications raccordés les uns aux autres par des routeurs périphériques (ou « edge routers ») ou des routeurs de frontière (ou « border routers »). Un tel établissement ne pose généralement pas de problème lorsque la communication n'est pas associée à un niveau de service particulier, ou lorsque la continuité du service associé à la communication n'est pas requise. Mais, cette dernière situation est de moins en moins fréquente du fait de la grande disparité des réseaux et de leurs équipements.

15

En effet, parmi les équipements de réseau couramment utilisés et susceptibles de coexister lors d'une communication, on peut notamment citer les routeurs IP, les routeurs à multiplexage de longueurs d'onde, tels que les dispositifs DWDM, les multiplexeurs d'insertion/extraction (ou ADMs pour « Add-Drop Multiplexors »), les brasseurs photoniques (ou PXC pour « Photonic Cross Connects »), ou les brasseurs optiques (ou OXC pour « Optical Cross Connects »).

20

25

De même, parmi les réseaux couramment utilisés et susceptibles d'être impliqués dans une communication, on peut notamment citer ceux qui appartiennent à la première famille des réseaux dits « à commutation de paquets » et ceux qui appartiennent à la seconde famille des réseaux dits « à commutation de niveau non paquet » (ou « none-packet switching »).

30

Les réseaux de la première famille utilisent des protocoles de niveau 3 dans le modèle en couches OSI (également appelés protocoles de niveau

IP, ou plus simplement protocoles Internet (ou IP)). Ils constituent ce que l'on a l'habitude d'appeler l'Internet.

Les réseaux de la seconde famille utilisent des protocoles de niveau 2 dans le modèle en couches OSI (également appelés protocoles de niveau sous-IP (ou « sub-IP »)). La seconde famille peut en outre être subdivisée en au moins trois sous-familles. Une première sous-famille est constituée des réseaux à commutation spatiale, une deuxième sous-famille est constituée des réseaux à multiplexage temporel (ou TDM pour « Time Division Multiplexing »), comme par exemple les réseaux SONET et SDH, et une troisième sous-famille est constituée des réseaux à multiplexage de longueurs d'onde (ou WDM pour « Wavelength Division Multiplexing »).

Afin de permettre l'établissement de communications via des réseaux IP différents (appartenant à la première famille), il a été proposé de raccorder chaque système de gestion de réseau (ou NMS pour « Network Management System »), qui gère les équipements d'un réseau IP, à un dispositif de contrôle d'admission de niveau réseau. Un tel dispositif de contrôle est chargé, lorsqu'il reçoit une demande de transfert, via son réseau IP, d'un appel associé à au moins un critère de service et désignant un autre réseau IP raccordé à son propre réseau IP, de vérifier s'il existe des ressources disponibles qui satisfont au(x) critère(s) de service associé(s) à l'appel à transférer. Ainsi, lorsque de telles ressources existent, le dispositif de contrôle peut adresser à son tour la demande de transfert d'appel au dispositif de contrôle qui est raccordé au système de gestion de réseau chargé de gérer les équipements du réseau IP désigné, de sorte qu'il puisse procéder à une éventuelle vérification au sein de son propre réseau IP.

On entend ici par « demande de transfert d'appel via un réseau », le fait d'établir au sein d'un premier réseau un « pont » entre deux autres réseaux, en mettant à disposition certaines ressources de l'une des liaisons de ce premier réseau.

Grâce à ce type de dispositif de contrôle, il est donc possible de garantir la continuité et la qualité du service associé à une communication lorsque les réseaux IP impliqués dans cette communication sont différents. Mais, il est également possible de garantir à un abonné la sécurité du service,

laquelle consiste à authentifier et/ou crypter une communication.

Mais, il n'existe pas de solution connue permettant de garantir la continuité et la qualité du service, ainsi qu'éventuellement la sécurité du service, associés à une communication lorsque l'établissement de cette
5 communication implique des réseaux de types différents, c'est-à-dire appartenant à des sous-familles de la seconde famille (dite famille sous-IP) ou à des familles différentes.

L'invention a donc pour but de remédier à cet inconvénient.

Elle propose à cet effet un dispositif dédié au contrôle d'admission de
10 niveau réseau pour un premier réseau de communications à protocole de niveau sous-IP (c'est-à-dire appartenant à la seconde famille précitée), comportant des routeurs de frontière, raccordés entre eux par des liaisons associées à des ressources de caractéristiques connues, et gérés par un premier système de gestion de réseau (ou NMS).

15 Ce dispositif de connexion se caractérise par le fait qu'il comprend des moyens de contrôle, d'une part, alimentés par le système de gestion de réseau en données d'information représentatives des liaisons entre les routeurs de frontière du premier réseau sous-IP et des ressources associées, et d'autre part, capables, lorsqu'ils reçoivent une demande de transfert, via le
20 premier réseau sous-IP, d'un appel qui est associé à au moins un critère de service et qui désigne un second réseau de communications raccordé au premier réseau sous-IP et d'un type différent (IP ou sous-IP), de déterminer parmi les données d'information reçues s'il existe des ressources réseau disponibles satisfaisant au(x) critère(s) de service associé(s) à l'appel à
25 transférer, et dans l'affirmative d'adresser la demande de transfert d'appel à un autre dispositif de contrôle raccordé au système de gestion de réseau (NMS) qui gère le second réseau désigné.

Ainsi, il est désormais possible de garantir la continuité du service et la qualité du service, ainsi qu'éventuellement la sécurité du service (cryptage
30 et/ou authentification), associés à une communication lorsque l'établissement de cette communication implique des réseaux de types différents, c'est-à-dire appartenant à des sous-familles de la seconde famille ou à des familles différentes.

Préférentiellement, le critère de service est choisi dans un groupe comprenant au moins la qualité de service, l'aptitude à la protection/restauration de liaison, et la sécurité du service.

5 Egalement de préférence, les moyens de contrôle peuvent être agencés de manière à stocker dans une mémoire les données d'information reçues, sous la forme d'une matrice de connectivité entre les différents routeurs de frontière du premier réseau sous-IP (c'est cette mémoire qui sera consultée pour savoir si suffisamment de ressources sont disponibles dans le réseau sous-IP pour le service désiré).

10 Par ailleurs, les moyens de contrôle du dispositif selon l'invention sont préférentiellement susceptibles d'être couplés à un autre dispositif de contrôle, raccordé au système de gestion de réseau (NMS) qui gère un troisième réseau de communications raccordé au premier réseau sous-IP et d'un type différent (IP ou sous-IP), et duquel est issu la demande de transfert d'appel.

15 L'invention porte également sur un équipement de réseau, comme par exemple un serveur, susceptible d'être raccordé à un système de gestion de réseau (NMS) gérant un réseau de communications à protocole de niveau sous-IP, et équipé d'un dispositif de contrôle d'admission de niveau réseau du type de celui présenté ci-avant.

L'invention s'applique tout particulièrement, bien que de façon non restrictive, aux réseaux de communications sous-IP choisis parmi les réseaux à commutation spatiale, les réseaux à commutation de longueurs d'onde (WDM), les réseaux TDM, et en particulier les réseaux SONET et SDH, et les réseaux GMPLS (pour « Generalized MultiProtocol Label Switching »).

25 D'autres caractéristiques et avantages de l'invention apparaîtront à l'examen de la description détaillée ci-après, et de l'unique figure annexée qui illustre de façon schématique un exemple d'installation de communications équipée d'un dispositif de contrôle selon l'invention. Cette figure pourra non seulement servir à compléter l'invention, mais aussi contribuer à sa définition, le cas échéant.

30 L'installation de communications illustrée, à titre d'exemple, sur l'unique figure comporte trois réseaux de communications de types différents.

Plus précisément, dans cet exemple l'installation comporte tout d'abord un premier réseau public de données, à protocole de niveau 3 selon le modèle OSI (ou protocole de niveau IP), ci-après appelé premier réseau IP (NIP1), un deuxième réseau public de données, également à protocole de niveau 3
5 selon le modèle OSI, ci-après appelé second réseau IP (NIP2), et éventuellement d'un type différent de NIP1, et un troisième réseau public de données, à protocole de niveau 2 selon le modèle OSI (ou protocole de niveau sous-IP), ci-après appelé réseau sous-IP (NSIP).

Par exemple, le réseau sous-IP NSIP est un réseau à multiplexage
10 temporel (ou TDM pour « Time Division Multiplexing »), comme par exemple un réseau SONET ou SDH. Mais, il pourrait s'agir de tout autre type de réseau sous-IP de niveau 2, comme par exemple un réseau à commutation spatiale ou un réseau à multiplexage de longueurs d'onde (ou WDM pour « Wavelength Division Multiplexing »), ou d'un réseau sous-IP de niveau dit
15 2,5, comme par exemple un réseau GMPLS (pour « Generalized MultiProtocol Label Switching »).

Le premier réseau IP NIP1 est géré par un système de gestion de réseau (NMS1) de type NMS, couplé à un serveur dit « de contrôle d'admission de niveau réseau » S1, également appelé contrôleur d'admission
20 de niveau réseau. Ce serveur S1 est chargé de vérifier, chaque fois qu'il reçoit une demande requérant le transfert d'un appel via le premier réseau IP NIP1, associé à au moins un critère de service et désignant un autre réseau (ici NSIP) raccordé au premier réseau IP NIP1, s'il existe des ressources réseau disponibles, associées aux différentes liaisons précédemment établies (par le
25 NMS1) au sein du premier réseau IP NIP1 entre ses différents routeurs, qu'ils soient de type « périphériques » (« edge routers ») ER1 ou de type « de frontière » (« border routers ») BR1, qui satisfont au(x) critère(s) de service associé(s) à l'appel à transférer.

Le second réseau IP NIP2 est géré par un système de gestion de
30 réseau (NMS2) de type NMS, couplé à un serveur de contrôle d'admission de niveau réseau S2, chargé de vérifier, chaque fois qu'il reçoit une demande requérant le transfert d'un appel via le second réseau IP NIP2, associé à au moins un critère de service et désignant un autre réseau raccordé au second



réseau IP NIP2, s'il existe des ressources réseau disponibles, associées aux différentes liaisons précédemment établies (par le NMS2) au sein du premier réseau IP NIP2 entre ses différents routeurs, qu'ils soient de type « périphériques » (« edge routers ») ER2 ou de type « de frontière » (« border routers ») BR2, qui satisfont au(x) critère(s) de service associé(s) à l'appel à transférer.

On entend ici par « critère de service » tout ce qui a trait au service associé à un appel, et notamment la qualité de service ou l'aptitude à assurer la continuité du service (également appelée protection / restauration) en cas de problème survenu sur une liaison, ou encore la sécurité du service.

La qualité de service (ou QoS) est définie par les caractéristiques d'une ressource, comme par exemple la bande passante offerte ou le niveau de qualité de service (or, argent ou bronze) offert. Ces niveaux de qualité de service résultent d'une classification faite à partir d'un certain nombre de paramètres tels que la bande passante, le délai, la gigue, les pertes, et analogues.

La continuité du service est définie par des paramètres tels que la capacité à pouvoir se protéger d'une discontinuité de service. Concrètement, lors d'un transfert de données, il est habituel de réclamer, en cas de « coupure », une protection / restauration mise en place en moins de 50 ms, par exemple.

La sécurité est la capacité de crypter et/ou d'authentifier une connexion entre deux points d'une matrice de connexion. Il est rappelé ici que la sécurité est considérée comme une ressource réseau. Par ailleurs, c'est le NMSi qui est chargé d'informer le serveur de contrôle Si de la possibilité de crypter et/ou d'authentifier une communication entre deux points de la matrice de connexion.

Chaque NMSi de réseau IP NIPi (ici $i = 1$ et 2) alimente, de façon statique (notamment dans des phases pré-opérationnelles), le serveur de contrôle Si correspondant en données d'information représentatives des liaisons établies entre les différents routeurs périphériques ERi et de frontière BRi du réseau IP NIPi et des ressources associées à ces liaisons. Ces données permettent ensuite au serveur de contrôle Si de mémoriser l'état

d'occupation des ressources de son réseau IP en fonction des demandes de service reçues. Par ailleurs, le NMSi informe régulièrement le serveur de contrôle Si de sorte qu'il puisse aligner sa connaissance de l'état des ressources avec les ressources réelles du réseau IP. Ainsi, chaque serveur
5 de contrôle Si sait à chaque instant quelles ressources sont disponibles dans le réseau IP NIPi qu'il contrôle.

Le réseau sous-IP NSIP est géré par un système de gestion de réseau (NMS3) de type NMS, couplé à un dispositif de contrôle d'admission de niveau réseau D, ici implanté dans un serveur de contrôle S3 raccordé aux
10 serveurs de contrôle S1 et S2 des premier NIP1 et second NIP2 réseaux IP.

Par ailleurs, le réseau sous-IP NSIP est raccordé à des routeurs de frontière BRi des premier NIP1 et second NIP2 réseaux IP par l'intermédiaire de certains de ses routeurs de frontière BR3-k (ici k = 1 et 2).

Le dispositif de contrôle D selon l'invention comprend une mémoire M
15 alimentée par le NMS3 du réseau sous-IP NSIP en données d'information réseau représentatives des liaisons établies entre les différents routeurs de frontière BR3-k (ici k = 1 et 2) du réseau sous-IP NSIP et des ressources associées à ces liaisons. Il est important de noter que cette alimentation de la mémoire se fait selon un mode de type « off line », indépendamment des
20 demandes de vérification de disponibilité de ressources ou des appels. Comme indiqué précédemment, l'alimentation est effectuée dans une phase pré-opérationnelle, mais également de temps en temps pendant toute la durée de vie du réseau concerné.

Par ailleurs, certaines données d'information réseau qui alimentent la
25 mémoire M peuvent désigner le mode de gestion d'une liaison par le serveur NMS3. Parmi ces modes de gestion on peut notamment citer « VPN » (pour « Virtual Private Network »), « Optical VPN » et « IPSec ».

On stocke également dans la mémoire M les données de restauration qui définissent les ressources réseau destinées à remplacer d'autres
30 ressources réseau en cas de problème.

Préférentiellement, les données d'information sont stockées dans la mémoire M sous la forme d'une matrice de connectivité définissant toutes les liaisons établies entre les différents routeurs de frontière BR3-k du réseau



sous-IP NSIP, et les ressources associées à ces liaisons ainsi que leurs caractéristiques et leurs états respectifs de disponibilité, mais également les liaisons de restauration et les ressources associées.

Le dispositif de contrôle D selon l'invention comprend également un module de contrôle CM couplé à la mémoire M et chargé de vérifier dans la matrice de connectivité de la mémoire M, chaque fois qu'il reçoit une demande requérant le transfert d'un appel via le réseau sous-IP NSIP, associé à au moins un critère de service et désignant un autre réseau (ici NSIP1 ou NSIP2) raccordé au réseau sous-IP NSIP, s'il existe des ressources disponibles, associées aux différentes liaisons précédemment établies au sein du réseau sous-IP NSIP entre ses routeurs de frontière (ou « border routers ») BR3-k, qui satisfont au(x) critère(s) de service associé(s) à l'appel à transférer.

Le module de contrôle D est capable de prendre en compte la signalisation propre aux réseaux sous-IP, qui provient d'un serveur d'appels multimédia (ou MMCS pour « MultiMedia Call Server ») ou d'un autre module de contrôle (ou serveur de contrôle Si) d'un réseau voisin auquel son réseau sous-IP est raccordé. Il est également capable de prendre en compte des données de protection / restauration dédiées aux réseaux sous-IP et des informations provenant de matrices de communications bidirectionnelles.

Le module de contrôle CM, ainsi qu'éventuellement la mémoire M, peuvent être réalisés sous la forme de circuits électroniques (ou « hardware »), de modules logiciels ou informatiques (ou « software »), ou d'une combinaison de circuits et de logiciels.

On va maintenant décrire un exemple d'utilisation de l'installation de communications illustrée sur l'unique figure. Dans cet exemple, on suppose qu'un premier terminal de communication T1 souhaite échanger des données, par exemple de type multimédia avec l'assurance de la continuité du service, avec un second terminal de communication T2.

On suppose par ailleurs que les premier T1 et second T2 terminaux sont raccordés à des réseaux de téléphonie public (non représentés), par exemple de type PLMN (pour « Public Land Mobile Network »), tel qu'un réseau UMTS ou i-Mode. Mais, dans une variante, ils pourraient être

raccordés à un réseau de type commuté (par exemple RTC pour « Réseau Téléphonique Commuté » ou PSTN pour « Public Switched Telephony Network »), voire même directement à un réseau IP.

On suppose en outre que les terminaux T1 et T2 sont des téléphones
5 mobiles. Mais, il pourrait s'agir, par exemple, d'ordinateurs fixes ou portables, de téléphones fixes, ou d'assistants personnels numériques (ou PDA pour « Personal Digital Assistant »), ou encore de tout type de terminal de communication capable d'échanger des données avec un autre terminal.

Le premier terminal T1 adresse initialement à son réseau de
10 téléphonie UMTS1 une requête demandant l'établissement d'une communication avec le second terminal T2, en vue d'échanger des données multimédia avec l'assurance d'une continuité de service. Le réseau UMTS1 initie alors une procédure destinée à déterminer si le second terminal T2 est disponible, et dans cette hypothèse le chemin qui permettrait d'établir la
15 communication avec ce second terminal T2 tout en satisfaisant aux deux critères de service requis.

Il interroge pour ce faire son serveur MMCS1 qui agit selon le niveau de signalisation, appelé niveau d'appel (ou « call level »), chargé de s'assurer de la compatibilité des deux terminaux T1 et T2 et des services qui leurs sont
20 associés avant d'essayer d'établir une connexion (il est en effet inutile d'essayer d'établir une connexion si le terminal distant (ici T2) est occupé ou si le service demandé par le terminal T1 n'est pas disponible, par exemple).

On suppose que dans l'exemple décrit, le serveur MMCS1 s'est assuré, par une procédure de signalisation au niveau d'appel, des
25 disponibilités du second terminal T2 et du service requis par le premier terminal T1. Par conséquent, il doit initier, par une procédure de signalisation au niveau de connexion, une vérification de la disponibilité des ressources. Pour ce faire, il se connecte au serveur de contrôle S1, du premier réseau IP NIP1, afin de lui demander de vérifier s'il dispose de ressources disponibles
30 qui satisfont aux deux critères de service requis par le premier terminal T1 et qui permettraient le transfert de l'appel vers le réseau sous-IP NSIP. Dans l'exemple illustré, le serveur de contrôle S1 s'aperçoit, en interrogeant sa matrice de connectivité, que certaines ressources de la liaison établie entre le

routeur périphérique ER1 et le routeur de frontière BR1 satisfont aux deux critères de service requis.

Le serveur de contrôle S1, sachant que son réseau IP NIP1 est raccordé au réseau sous-IP NSIP, transmet à son serveur de contrôle S3 la
5 demande de vérification de disponibilité de ressources satisfaisant aux deux critères de service requis par le premier terminal T1 et permettant le transfert de l'appel vers le second réseau IP NIP2.

Cette demande de vérification est traitée par le module de contrôle CM du dispositif de contrôle D implanté dans le serveur de contrôle S3. Le
10 module de contrôle CM interroge alors la matrice de connectivité qui est stockée dans la mémoire M, et s'aperçoit, dans l'exemple illustré, que certaines ressources de la liaison établie entre les routeurs de frontière BR1-3 et BR2-3 satisfont aux deux critères de service requis.

Le module de contrôle CM, sachant que son réseau sous-IP NSIP est
15 raccordé au réseau IP NIP2, charge le serveur de contrôle S3 de transmettre au serveur de contrôle S2, du second réseau IP NIP2, la demande de vérification de disponibilité de ressources satisfaisant aux deux critères de service requis par le premier terminal T1 et permettant le transfert de l'appel vers le réseau UMTS2.

Dans l'exemple illustré, le serveur de contrôle S2 s'aperçoit, en
20 interrogeant sa matrice de connectivité, que certaines ressources de la liaison établie entre le routeur de frontière BR2 et le routeur périphérique ER2 satisfont aux deux critères de service requis.

Préférentiellement, en cas de disponibilité des ressources, il n'est pas
25 nécessaire que le serveur de contrôle S2 avertisse le serveur MMCS2 du réseau UMTS2. Il est préférable que cet avertissement soit adressé au serveur MMCS1 en cas d'indisponibilité des ressources. Dans cette situation, le serveur MMCS1 signale ensuite au serveur MMCS2 que la connexion ne peut pas se faire.

Dans l'exemple illustré, les ressources étant disponibles au niveau
30 des trois réseaux de transfert (ou transit) impliqués (NIP1, NSIP et NIP2), le serveur MMCS2 en informe le serveur MMCS1, lequel en informe le réseau UMTS1. Bien entendu, lorsque le premier terminal T1 est directement

raccordé au réseau IP NIP1, le MMCS1 informe directement T1 qu'il peut se connecter au second terminal T2. Cela met fin à la procédure de vérification de disponibilité de ressources.

5 Les ressources satisfaisant aux deux critères de service étant disponibles au sein des trois réseaux qui sont ici impliqués (NIP1, NSIP et NIP2), la connexion entre les premier T1 et second T2 terminaux peut être établie via le routeur périphérique ER1 et le routeur de frontière BR1 du premier réseau IP NIP1, les routeurs de frontière BR3-1 et BR3-2 du réseau sous-IP NSIP, et le routeur de frontière BR2 et le routeur périphérique ER2 du
10 second réseau IP NIP2.

La procédure d'établissement de la communication est alors terminée et les deux terminaux T1 et T2 peuvent commencer à échanger des données multimédia en ayant l'assurance de bénéficier de la continuité du service pendant toute la durée de la communication. En effet, en cas de problème sur
15 l'une des liaisons, ils ont la garantie que le réseau de transfert concerné (NIP1, NSIP ou NIP2) mettra immédiatement à leur disposition des ressources équivalentes. En d'autres termes, grâce à l'invention la continuité du service associé à un appel est effectivement assurée sur l'intégralité du chemin reliant un terminal appelant à un terminal appelé, et cela quel que soit
20 le nombre de réseaux de transfert (ou transit) impliqués.

L'invention ne se limite pas au mode de réalisation d'installation, de dispositif de contrôle et de serveur de contrôle décrits ci-avant, seulement à titre d'exemple, mais elle englobe toutes les variantes que pourra envisager l'homme de l'art dans le cadre des revendications ci-après.

25 Ainsi, l'invention est ni limitée à l'exemple illustré de combinaison de réseaux de téléphonie et de réseaux de données, ni au nombre de réseaux choisis, dès lors qu'au moins deux des réseaux de données sont de types différents et que l'un au moins d'entre eux est un réseau sous-IP.

REVENDICATIONS

1. Dispositif de contrôle d'admission de niveau réseau (D), pour un premier réseau de communications à protocole de niveau dit « sous-IP »
5 (NSIP) comportant des routeurs de frontière (BR3-k), raccordés entre eux par des liaisons associées à des ressources de caractéristiques connues, et gérés par un premier système de gestion de réseau (NMS3), caractérisé en ce qu'il comprend des moyens de contrôle (CM) alimentés par ledit système de gestion de réseau (NMS3) en données d'information représentatives
10 desdites liaisons entre routeurs de frontière (BR3-k) dudit réseau et des ressources associées, et agencés, en cas de réception d'une demande de transfert, via ledit réseau (NSIP), d'un appel associé à au moins un critère de service et désignant un second réseau de communications (NIP2) raccordé audit premier réseau et d'un type différent, à déterminer parmi lesdites
15 données d'information si il existe des ressources disponibles satisfaisant au critère de service associé audit appel à transférer, et dans l'affirmative adresser ladite demande de transfert d'appel à un second dispositif de contrôle (S2) raccordé à un second système de gestion de réseau (NMS2) gérant ledit second réseau désigné (NIP2).
- 20 2. Dispositif selon la revendication 1, caractérisé en ce que ledit critère de service est choisi dans un groupe comprenant au moins la qualité de service, l'aptitude à la protection / restauration de liaison, et la sécurité.
3. Dispositif selon la revendication 2, caractérisé en ce que ladite qualité de service est définie par au moins un paramètre choisi dans un
25 groupe comprenant au moins la bande passante, le délai, les pertes et la gigue.
4. Dispositif selon l'une des revendications 1 à 3, caractérisé en ce que certaines desdites données d'information désignent un mode de gestion d'une liaison par ledit système de gestion de réseau (NMS3).
- 30 5. Dispositif selon la revendication 4, caractérisé en ce que lesdits modes sont choisis dans un groupe comprenant au moins VPN, Optical VPN et IPSec.
6. Dispositif selon l'une des revendications 2 à 5, caractérisé en ce que

certaines desdites données d'information définissent des liaisons de restauration et des ressources associées.

5 7. Dispositif selon l'une des revendications 1 à 6, caractérisé en ce qu'il comprend une mémoire (M), et en ce que lesdits moyens de contrôle (CM) sont agencés pour stocker dans ladite mémoire (M) les données d'information reçues, sous la forme d'une matrice de connectivité entre routeurs de frontière (BR3-k) du premier réseau (NSIP).

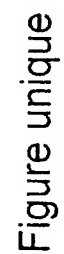
10 8. Dispositif selon l'une des revendications 1 à 7, caractérisé en ce que lesdits moyens de contrôle (CM) sont propres à être couplés à un troisième dispositif de contrôle (S1), raccordé à un troisième système de gestion de réseau (NSMS1), gérant un troisième réseau de communications (NIP1) raccordé au premier réseau sous-IP (NSIP) et d'un type différent, et duquel est issu ladite demande de transfert d'appel.

15 9. Dispositif selon l'une des revendications 1 à 8, caractérisé en ce que l'un au moins desdits second (NIP2) et troisième (NIP1) réseaux est à protocole de niveau IP.

10 10. Dispositif selon l'une des revendications 1 à 9, caractérisé en ce que l'un au moins desdits second (NIP2) et troisième (NIP1) réseaux est à protocole de niveau sous-IP.

20 11. Equipement de réseau (S3) propre à être raccordé à un système de gestion de réseau (NMS3) gérant un réseau de communications à protocole de niveau sous-IP (NSIP), caractérisé en ce qu'il comprend un dispositif de contrôle d'admission de niveau réseau (D) selon l'une des revendications 1 à 10.

25 12. Utilisation du dispositif de contrôle d'admission de niveau réseau (D) et de l'équipement de réseau (S3) selon l'une des revendications précédentes, dans les réseaux de communications sous-IP choisis dans un groupe comprenant les réseaux à commutation spatiale, les réseaux à commutation de longueur d'onde, les réseaux TDM, et les réseaux GMPLS.





DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg

75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1./1..

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 2608

| | | | |
|---|----------------------|---|------------------|
| Vos références pour ce dossier <i>(facultatif)</i> | | 104572/SYC/NBND/TPM | |
| N° D'ENREGISTREMENT NATIONAL | | 0216227 4 | |
| TITRE DE L'INVENTION (200 caractères ou espaces maximum) DISPOSITIF DE CONTROLE D'ADMISSION DE NIVEAU RESEAU POUR UN RESEAU DE COMMUNICATIONS A PROTOCOLE DE NIVEAU SOUS-IP | | | |
| LE(S) DEMANDEUR(S) : Société anonyme ALCATEL | | | |
| DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages). | | | |
| Nom | | GALAND | |
| Prénoms | | Damien | |
| Adresse | Rue | 24, RUE DU PAVÉ DES GARDES | |
| | Code postal et ville | 92370 | CHAVILLE, FRANCE |
| Société d'appartenance <i>(facultatif)</i> | | | |
| Nom | | | |
| Prénoms | | | |
| Adresse | Rue | | |
| | Code postal et ville | | |
| Société d'appartenance <i>(facultatif)</i> | | | |
| Nom | | | |
| Prénoms | | | |
| Adresse | Rue | | |
| | Code postal et ville | | |
| Société d'appartenance <i>(facultatif)</i> | | | |
| DATE ET SIGNATURE(S) XX (RS) XX (RS) XX (RS) XX DU MANDATAIRE (Nom et qualité du signataire) | | 13 novembre 2002 Sylvain CHAFFRAIX | |

THIS PAGE BLANK (USPTO)